



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,165	03/17/2004	James D. Gersten	ELYN/10	4146
26875	7590	04/20/2007	EXAMINER	
WOOD, HERRON & EVANS, LLP 2700 CAREW TOWER 441 VINE STREET CINCINNATI, OH 45202			TRAORE, FATOUUMATA	
			ART UNIT	PAPER NUMBER
			2109	
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE		DELIVERY MODE	
3 MONTHS	04/20/2007		PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/802,165	GERSTEN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Fatoumata Traore	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 17 March 2004.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-37 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 17 March 2004 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>6/16/2004</u> .   | 6) <input type="checkbox"/> Other: _____ .                        |

### **DETAILED ACTION**

1. This action is in response of the original filing of March 17, 2004. Claims 1-38 are pending and have been considered below.

#### **Claim Objections**

2. Claims 11, 30 are objected to because of the following informalities: the examiner notes the use of acronyms (e.g. PCL) throughout the claims without first including a description in plain text, as required.

Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 101***

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 36, 37 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 36 and 37 are drawn to a signal-bearing medium, which the applicant has defined in the specification (page 12, lines 3-11) to encompass an electronic transmission signal. The Office considers an electronic signal to be a form of energy. Energy is not a series of steps or acts and this is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a

compilation of matter. Thus, an electronic transmission signal does not fall within any of the four categories of invention. Therefore, Claims 36 and 37 are not statutory.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 16, 18 are rejected under 35 U.S.C. 102(b) as being anticipated by Michael (US 2002/0188689).

Claim 16: Michael discloses a method for secure electronic mail transfer comprising:

Generating at a local computer using a non-browser application configured for electronic transmission that includes an electronic mail analogous interface, an encrypted package comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the

name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107);  
And transmitting from the local computer the package over a secure network connection over the public Internet (the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161).

Claim 18: Michael discloses a method for secure electronic mail transfer as in claim 16 above, and further discloses a step of communicating the package to the addressee (if sender is authenticated, the email message will be delivered to recipient's mailbox and will be accessible to recipient's email application) (page 12, paragraph 164)

#### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-10, 12, 13, 17-21, 23-29, 31, 33-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Michael (US 2002/0188689) in view of Benninghoff (US 2002/0091782).

Claim 1: Michael discloses a method for secure electronic mail transfer comprising:

- i. Generating a package using a non-browser application on a local computer, the package configured for electronic transmission that includes an electronic mail analogous interface, file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107);
- ii. Communicating the package from the local computer to a secure server over a secure network connection over the public Internet (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key) (page 12, paragraph 161);

- iii. Communicating the package to the addressee (if sender is authenticated, the email message will be delivered to recipient's mailbox and will be accessible to recipient's email application) (page 12, paragraph 164);
- iv. Decrypting the package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161);
- v. And displaying the package to the addressee (the recipient's destination application recognizes the header bearing email and displays such) (page 9, paragraph 07).

Michael does not disclose that the package is stored at the server. However, Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 17: Michael discloses a method for secure electronic mail transfer as in claim 16 above, but does not explicitly disclose that the package is stored at the server. However, Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 21: Michael discloses an apparatus for secure electronic mail transfer comprising:

- i. A computer (page 1, paragraph 6);
- ii. A program code in communication with at least one of the local and server computers, the program code configured to generate a package using a non-browser application on the local computer, the package being configured for electronic transmission that includes an electronic mail analogous interface, file data and an address associated with an addressee having a public electronic mail account (the present invention,

graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code being further configured to communicate the package from the local computer to the secure server over the secure network connection (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key) (page 12, paragraph 161), and to store the package at the server in association with the electronic mail account of the addressee, the program code being further configured to decrypt (the receiver can decrypt the email using sender private key) (page 12, paragraph 161) and communicate the package to the addressee the recipient's destination application recognizes the header bearing email and displays such) (page 9, paragraph 07).

Michael does not disclose: the package is stored at the server; a server computer;

However, Benninghoff discloses a method of verifiably transmitting an electronic package, which further discloses

A server computer configured to communicate with the local computer over a secure network connection (figure 1);

And a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125).

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step storing the electronic package at the server to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claims 2, 23: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and Michael further discloses that the package is encrypted at the local computer of a sender (the sender can encrypt the email using their public key) (page 12, paragraph 161).

Claims 3, 24: Michael, and Benninghoff disclose a method and system for secure electronic mail transfer as in claims 2 and 23 above, and Michael further discloses that the step of encrypting the package at the local computer of the sender further includes using a public key to encrypt the package (the sender can encrypt the email using their public key) (page 12, paragraph 161).

Claims 4, 25: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and Michael further discloses that the step of decrypting the package further includes using a private key associated with a public key previously used to encrypt the package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161).

Claims 5, 26: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and Benninghoff discloses a method and apparatus of verifiably transmitting an electronic package, which further discloses a step of storing the package as a draft package at the local computer prior to communicating the package to the secure server (the invention provides a system and method where any person may caused to be transmitted electronically files in electronic format and register electronically with PoS-e the time, date, file size, sender, and recipient of said transmission and provide that a duplicate of the transmitting message be stored on PoS-e's server for a designated period of time) (page 4, paragraph 60).

Therefore, it would have been obvious for one having ordinary skill in the art at

the time the invention was made to add a step of storing the package as a draft to Michael's teaching. One would have been motivated to do so in order to allow the user to complete the package at a later time.

Claims 6, 27: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and Benninghoff discloses a method and apparatus of verifiably transmitting an electronic package which further discloses a step of causing the addressee to be notified of the package using the public electronic mail account (the server sends an email notification to the recipient indicating that an electronic package addressed to the recipient is available on the server) (page 8, paragraph 133). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of notifying the addressee in Michael's teaching. One would have been motivated to do so in order to allow the addressee to access the package.

Claims 7, 28: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and Michael further discloses that communicating the package to the addressee further includes communicating the package using at least one of the secure network connection and a second secure network connection (the sender signs the emails using their private key, the recipient server can verify the sender information the email using sender's public key) (page 12, paragraph 161).

Claim 8: Michael, and Benninghoff disclose a method for secure electronic mail transfer as in claim 1 above, and Benninghoff discloses a method and apparatus of verifiably transmitting an electronic package which further discloses a step of configuring the interface to be responsive to user input (at step 142, via the sender's client-side application, the system display various PoS-e services that may be selected by sender as is appropriate to his circumstances) (page 7, paragraph 126). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of getting user input to Michael's teaching. One would have been motivated to do so in order to allow the user to enter or change data in the package.

Claims 9, 29: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and Benninghoff discloses a method and apparatus of verifiably transmitting an electronic package, which further discloses a step of configuring the interface to display a status of the package (Figure 27). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of configuring the interface to display status of the package to Michael's teaching. One would have been motivated to do so in order to allow the sender to determine when the package was delivered.

Claim 10: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claim 1 above, and Michael further discloses a step of adding additional file data to the package (hyperlinks or other resources

are attached to the header, including a typical email body) (page 9, paragraph 107).

Claim 12: Michael, and Benninghoff disclose a method for secure electronic mail transfer as in claim 1 above, and Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses a step of downloading the package from the secure server (the recipient download the contents of the electronic package that was prepared and transmitted by the subscriber) (page 8, paragraph 134). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step downloading the package to Michael's teaching. One would have been motivated to do so in order to allow the receiver to access the package.

Claims 13, 31: Michael, and Benninghoff disclose a method for secure electronic mail transfer as in claims 1 and 21 above, and Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses a step of automatically downloading the package from the secure server (the server presents the recipient with a download page like that shown in fig 11. which allows the recipient to elect delivery of the electronic package by either downloading it with a java applet, by downloading directly, or by receiving it as an encrypted email attachment ) (page 8, paragraph 134). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step downloading the package to Michael's teaching. One would

have been motivated to do so in order to allow the receiver to access the package.

Claim 19: Michael discloses a method for secure electronic mail transfer comprising:

- i. Receiving over a secure network connection over the public Internet a package, using a non-browser application that includes an electronic mail analogous interface, the package configured for electronic transmission and comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107),
- ii. Decrypting the package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161);

iii. And displaying the package to the addressee (the recipient's destination application recognizes the header bearing email and displays such) (page 9, paragraph 07).

Michael does not disclose that the package is stored at the server.

However, Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity

Claim 20: Michael discloses a method for secure electronic mail transfer comprising:

i. Generating a package for electronic transmission using a non-browser application that includes an electronic mail analogous interface (the present invention, graphical banner like display is used in lieu of the current arts inbox for text-based header for email. It is transported over the typical email protocols and displayed at the destination client. It can

be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107);

- ii. Encrypting the package (the sender can encrypt the email using their public key) (page 12, paragraph 161);
- iii. Communicating the package from the local computer to a secure server over a secure network connection over the public Internet wherein the package is stored at the server and communicated to an addressee (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161);

Michael discloses neither that the package is stored at the server nor communicating the delivery status of the package. However, Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and

Art Unit: 2109

use in generating the electronic certificate of service) (page 7, paragraph 125), which further discloses a step of causing the addressee to be notified of the package using the public electronic mail account (the server sends an email notification to the recipient indicating that an electronic package addressed to the recipient is available on the server) (page 8, paragraph 133). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server and a step of notification of the package status to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity

Claim 33: Michael discloses an apparatus for secure electronic mail transfer comprising:

- i. A computer (page 1, paragraph 6);
- ii. And program code in communication with the computer, the program code using a non-browser application and including an electronic mail analogous interface configured to receive from a remote computer over a secure network connection over the public Internet an encrypted package comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email

protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code being further configured to store the package in association with an electronic mail account of the addressee and to communicate the package to the addressee (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161).

Michael does not explicitly disclose that the package is stored at the server. However, Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to Michael's teaching. One would have

motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 34: Michael discloses an apparatus for secure electronic mail transfer comprising:

- i. A computer (page 1, paragraph 6);
- ii. And program code in communication with the computer, the program code configured to receive over a secure network connection over the public Internet a package generated using a non-browser application that includes an electronic mail analogous interface, the package being configured for electronic transmission and comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), wherein the package has been stored remotely at a secure server, the program code further configured to decrypt and display the package

(the receiver can decrypt the email using sender private key) (page 12, paragraph 161).

Michael does not explicitly disclose that the package is stored at the server. However, Benninghoff discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 35: Michael discloses an apparatus for secure electronic mail transfer comprising:

- i. A computer (page 1, paragraph 6);
- ii. And program code in communication with the computer, the program code configured to generate a package using a non-browser application that includes an electronic mail analogous interface, the package being configured for electronic transmission (the present invention, graphical banner like display is used in lieu of the current arts

inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code further being configured to encrypt the package and to communicate the package from the computer to a secure server over a secure network connection over the public Internet (the sender can encrypt the email using their public key) (page 12, paragraph 161), wherein the package is stored at the server and communicated to an addressee, wherein the program code is further configured to communicate a confirmation of delivery status of the package from the secure server to the non-browser application at the local computer via a secure network connection over the public Internet.

Michael does not explicitly disclose:

The package is stored at the server;

The program code is further configured to communicate a confirmation of delivery status of the package from the secure server.

However, Benninghoff discloses an apparatus of verifiably transmitting an electronic package, which further discloses a step of storing the package at the

server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125) and a step of communicating the status of package (the server sends an email confirmation to the sender indicating that the electronic package has been received by the server and is pending delivery to the recipient) (page 8, paragraph 133). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server and a step of notifying the sender to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 36: Michael discloses a program product for secure electronic mail transfer comprising:

- i. Program code in communication with at least one of a local and a server computer, the program code configured to generate a package using a non-browser application that includes an electronic mail analogous interface on the local computer, the package being configured for electronic transmission comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical

email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code being further configured to communicate the package from the local computer to the secure server over a secure network connection (the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161), and to store the package at the server in association with the electronic mail account of the addressee, the program code being further configured to decrypt and communicate the package to the addressee package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161);

- ii. And a signal bearing medium bearing the program code (the invention system may also be considered to be implemented as a computer readable storage medium) (page 1 paragraph 7).

Michael does not explicitly disclose that the package is stored at the server. However, Benninghoff discloses a method of verifiably transmitting an electronic

package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to Michael's teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 37: Michael, and Benninghoff disclose a program for secure electronic mail transfer as in claim 36 above, and Michael further discloses that the signal bearing medium includes at least one of a recordable medium and a transmission-type medium (such computer program is preferably stored on a storage media or device readable by general or special purpose programmable computer) (page 1, paragraph 7).

Claims 11, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Michael (US 2002/0188689) and Benninghoff (US 2002/0091782) in view of Maxwell (US 5805810).

Claims 11, 30: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, but do not disclose a

step of including a PCL file within the file data. However, Maxwell discloses a method and apparatus for converting electronic mail to a postal mail at the receiving station which further disclose the use of a PCL file within the file data (if the email contains sufficient information to generate a mail object, message validator provides the generated mail object to the print queue processor executing in the print server. The print queue processor then prints the mail object as postal mail) (column 5, lines 50-60). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step generating PCL file to Michael's teaching. One would have motivated to do so in order to ensure delivery of the package.

8. Claims 14, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Michael (US 2002/0188689) and Benninghoff (US 2002/0091782) in view of Montville et al (US 6356937).

Claims 14, 32: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, but do not disclose a step of compressing at least a portion of the package. However, Maxwell discloses a method and apparatus fro converting electronic mail to a postal mail at the receiving station which further discloses a step of compressing at least a portion of the package (the user is given control over whether or not to compress the file size of each outgoing attachment to a message) (column 3, lines 65-67). Therefore, it would have been obvious for one having ordinary skill in the art at

the time the invention was made to add the step of compressing at least portion of the file to Michael's teaching. One would have motivated to do so in order to decrease the bandwidth needed to transmit the package.

9. Claims 15, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Michael (US 2002/0188689) and Benninghoff (US 2002/0091782) in view of Dye et al (US 2005/0114658).

Claims 15, 22: Michael, and Benninghoff disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, but do not explicitly disclose the use of https socket layer connection. However, Dye et al discloses a remote web site security system, which further disclose the use of a secure Https layer (figure 1). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to use a secure https connection in Michael's teaching. One would have motivated to do so in order to prevent unauthorized access to the package by third parties.

### ***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Callas et al (US 2004/0133774) System and method for dynamic data security operations.

- b. Williams (US 5675733) Statistical analysis and display of reception status of electronic mail messages.
- c. King et al (US 2002/0002590) System and method for sending electronic mail and parcel delivery notification using recipient identification information.
- d. Huang (US 2003/0231207) Personal e-mail system and method.
- e. Goldstone (US 2003/0142364) Encrypted email message retrieval system.
- f. Little et al (2004/0171369) Certificate management and transfer system and method.
- g. Sistla (US 2003/0126463) Method and apparatus for preserving confidentiality of electronic mail.
- h. Riddle (US 6968458) Apparatus and method for providing secure communication on a network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

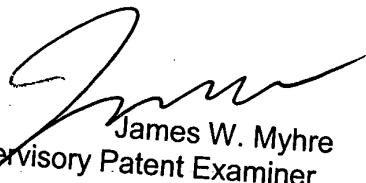
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Application/Control Number: 10/802,165  
Art Unit: 2109

Page 28

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT  
April 3, 2007



James W. Myhre  
Supervisory Patent Examiner